

| | | | | |
|--|---|------------------------|--------------|------------------|
|  metalkraft | PROCEDIMENTO (P) Política de Segurança da Informação para Fornecedores | Nº 27 | Norma | Requisito |
| | | | IATF 16949 | |
| | | | ISO 14001 | |
| | | | TISAX | x 1.1.1 |

1. OBJETIVO

Esta política tem como objetivo estabelecer diretrizes e responsabilidades relativas à segurança da informação no relacionamento entre a Metalkraft Sistemas Automotivos e seus fornecedores. Visa garantir a proteção dos ativos de informação da organização, promover a conformidade com leis e regulamentações (como a LGPD), prevenir riscos de segurança e preservar a integridade, disponibilidade e confidencialidade das informações.

2. APLICAÇÃO E RESPONSABILIDADE

Aplica-se a todos os fornecedores, parceiros, prestadores de serviço, consultores e terceiros que, de qualquer forma, tenham acesso, utilizem ou processem informações, sistemas, ambientes físicos ou lógicos, ou recursos da Metalkraft.

3. DEFINIÇÕES E ABREVIAÇÕES

Confidencialidade: garantia de que a informação é acessível apenas por pessoas autorizadas.

Disponibilidade: garantia de que usuários autorizados obtenham acesso às informações e ativos sempre que necessário.

Integridade: salvaguarda da exatidão e completude da informação e dos métodos de processamento.

Rastreabilidade: capacidade de rastrear o uso, alteração e movimentação das informações.

Responsabilidade: cada fornecedor é responsável por adotar boas práticas de segurança e comunicar falhas ou vulnerabilidades.

4. DESCRIÇÃO DAS ATIVIDADES

4.1. Diretrizes gerais para Fornecedores

- a) Informações Confidenciais: são todos os dados e conteúdos, de qualquer natureza, revelados ao fornecedor pela METALKRAFT, que não devem ser divulgados a terceiros.

| | | | | |
|--|---|------------------------|--------------|------------------|
|  metalkraft | PROCEDIMENTO (P) Política de Segurança da Informação para Fornecedores | Nº 27 | Norma | Requisito |
| | | | IATF 16949 | |
| | | | ISO 14001 | |
| | | | TISAX | x 1.1.1 |

Isso inclui:

- Dados pessoais e sensíveis (conforme a LGPD);
- Informações técnicas, operacionais, administrativas, comerciais ou jurídicas;
- Modelos de negócio, fórmulas, componentes, matéria-prima, projetos e escopos;
- Documentos, negociações e informações sobre clientes da METALKRAFT;
- Segredos comerciais e know-how;
- Conteúdos em qualquer formato: escrito, verbal, digital, gráfico, visual etc.;
- Tudo o que for compartilhado formal ou informalmente, direta ou indiretamente, por funcionários, sócios, parceiros ou clientes da METALKRAFT.

Em resumo: toda informação compartilhada no contexto da relação com a METALKRAFT é considerada confidencial e deve ser protegida.

- b) Utilizar os dados da Metalkraft exclusivamente para os fins acordados contratualmente, sob pena de responsabilização civil, contratual e penal.
- c) Adotar controles administrativos, técnicos e físicos que assegurem a proteção da informação em todo o seu ciclo de vida.
- d) Garantir conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e outras normativas relevantes (ex. ISO/IEC 27001, NIST, TISAX, etc.).
- e) Informar imediatamente à Metalkraft qualquer incidente de segurança, vazamento, perda ou violação de dados, inclusive dados pessoais.
- f) Submeter-se a auditorias e revisões técnicas sempre que solicitado pela Metalkraft, inclusive em suas próprias instalações.
- g) Assegurar que seus colaboradores, terceirizados e subfornecedores estejam devidamente treinados e cientes desta política.
- h) Nomear um responsável técnico pela segurança da informação como ponto de contato com a Metalkraft.
- i) Implementar políticas de acesso baseadas em perfil mínimo necessário (princípio do menor privilégio) e controle de senhas.
- j) Utilizar apenas softwares licenciados, ferramentas homologadas e infraestrutura aprovada para execução dos serviços.

| | | | | |
|---|---|------------------------|--------------|------------------|
|  metalkraft | PROCEDIMENTO (P) Política de Segurança da Informação para Fornecedores | Nº 27 | Norma | Requisito |
| | | | IATF 16949 | |
| | | | ISO 14001 | |
| | | | TISAX | x 1.1.1 |

- k) Adotar práticas de segurança como backups regulares, criptografia de dados sensíveis, e proteção contra malware e invasões.
- l) Garantir que, ao final da relação contratual, todos os dados, documentos e mídias com informações da Metalkraft sejam devolvidos ou destruídos de forma segura e auditável.
- m) Cumprir acordos de confidencialidade (NDA) e manter a confidencialidade das informações mesmo após o encerramento da relação contratual.

4.2. Classificação de Fornecedores

Os fornecedores serão classificados conforme o nível de criticidade das informações e sistemas acessados:

| Classificação | Tipo de Acesso à Informação |
|------------------|--|
| Alta (A) | Acesso a informações altamente sensíveis, como dados pessoais, financeiros, de saúde ou propriedade intelectual; acesso a sistemas críticos; falhas de segurança com impacto na reputação ou conformidade da empresa. Exemplos: administradores de domínio, consultores com acesso a projetos confidenciais. |
| Média (B) | Acesso a informações financeiras ou comerciais de sensibilidade moderada; acesso a sistemas ou redes que não comprometam criticamente a segurança. |
| Baixa (C) | Acesso a informações públicas ou de baixa sensibilidade; sem acesso a sistemas essenciais ou informações críticas. |

4.3. Monitoramento, sanções e consequências

A Metalkraft se reserva o direito de:

- Realizar auditorias, avaliações técnicas e revisões de segurança com ou sem aviso prévio;
- Solicitar planos de ação para tratamento de vulnerabilidades ou não conformidades;
- Aplicar sanções contratuais, legais ou administrativas, incluindo suspensão de fornecimento e rescisão contratual;
- Notificar autoridades competentes, caso aplicável.

O não cumprimento das diretrizes aqui estabelecidas poderá resultar em medidas disciplinares e legais conforme a gravidade da infração.

| | | | | |
|--|---|------------------------|--------------|------------------|
|  metalkraft | PROCEDIMENTO (P) Política de Segurança da Informação para Fornecedores | Nº 27 | Norma | Requisito |
| | | | IATF 16949 | |
| | | | ISO 14001 | |
| | | | TISAX | x 1.1.1 |

4.4. Tabela de exemplo de informações sensíveis.

| Categoria | Exemplos |
|-----------------------------------|--|
| Propriedade Intelectual | Patentes, segredos comerciais, inovações, projetos de P&D, know-how |
| Segredos Empresariais | Estratégias comerciais, planos de marketing, parcerias, informações operacionais |
| Informações Governamentais | Dados relacionados à defesa, segurança nacional, contratos públicos |
| Informações de Clientes | Dados de contato, projetos confidenciais, histórico de compras, preferências |
| Dados Pessoais | Nome, CPF, endereço, telefone, biometria, dados sensíveis conforme LGPD |
| Informações Médicas | Dados de saúde, históricos médicos, exames e tratamentos |
| Informações Profissionais | Histórico de empregos, salários, avaliações de desempenho |
| Informações Financeiras | Dados bancários, cartões de crédito, transações financeiras |
| Tecnologia da Informação | Senhas, acessos, backups, configurações de rede, códigos |
| Infraestrutura Crítica | Sistemas de energia, transportes, telecomunicações, datacenters |
| Informações Regulatórias | Licenças, certificações, relatórios de auditoria e conformidade |

4.5. Processo de avaliação de Fornecedores

Para garantir a conformidade com esta política e com os requisitos de segurança da informação, os fornecedores serão avaliados conforme os seguintes critérios e etapas:

a) Envio do FOR 192 - Avaliação de risco em segurança da informação e proteção de dados: A Metalkraft enviará ao fornecedor o FOR 192, elaborado com base na classificação de criticidade (alta, média ou baixa) atribuída ao fornecedor.

| | | | | |
|---|---|------------------------|--------------|------------------|
|  metalkraft | PROCEDIMENTO (P) Política de Segurança da Informação para Fornecedores | Nº 27 | Norma | Requisito |
| | | | IATF 16949 | |
| | | | ISO 14001 | |
| | | | TISAX | x 1.1.1 |

b) Prazo para Resposta: O fornecedor deverá responder o FOR 192, com envio de todas as evidências solicitadas, no prazo máximo de 30 dias corridos a partir do recebimento do documento.

c) Apresentação de Evidências: Juntamente com o FOR 192, o fornecedor deverá apresentar evidências documentais que comprovem a implementação das medidas declaradas, tais como procedimentos internos, registros de treinamentos, relatórios de auditoria interna, certificados ou capturas de tela.

d) Análise e Validação: A Metalkraft realizará a análise das informações e evidências enviadas e poderá, a seu critério, solicitar esclarecimentos adicionais, realizar visitas técnicas ou auditorias presenciais/remotas.

e) Plano de Ação Corretiva: Caso sejam identificadas não conformidades, o fornecedor deverá elaborar e apresentar um Plano de Ação contendo prazos, responsáveis e medidas corretivas. O não cumprimento do plano poderá acarretar restrições contratuais ou sanções.

f) Periodicidade: A reavaliação poderá ocorrer anualmente ou sempre que houver mudanças relevantes no escopo dos serviços, no ambiente do fornecedor, ou na legislação aplicável.

4.6. Disposições finais

Esta política será revista e atualizada sempre que necessário, em alinhamento com mudanças legais, contratuais ou tecnológicas. A adesão do fornecedor será formalizada mediante aceite por assinatura ou aceite digital.

5. DOCUMENTOS RELACIONADOS

- FOR-192 - Avaliação de risco em segurança da informação e proteção de dados

6. ALTERAÇÃO E APROVAÇÃO

| Revisão | Data | Elaborador | Aprovador | Resumo da alteração |
|---------|------------|------------------------------|-----------------------|---------------------|
| 00 | 25/08/2025 | João Dias de Oliveira Junior | Diovana Paula Barbosa | Emissão inicial |